UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of a 2012 Navistar International Truck bearing California (CA) license plate "FANNUM1" with vehicle identification number 1HSHXSJR2CJ624475 registered to Marck Gomez at 19122 East Elberland Street, West Covina, CA, 91792	Case No. 2:24-MJ-3732

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-3

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 549	Removing Goods from Customs Custody
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 545	Smuggling
18 U.S.C. § 542	Entry of Goods By Means of False Statement

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

Martina Doino, HSI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

The Hon. Alka Sagar, Magistrate Judge
Printed name and title

AUSA: Colin Scott (x3159)

ATTACHMENT A-3

VEHICLE TO BE SEARCHED

A 2012 Navistar International Truck bearing California (CA) license plate "FANNUM1" with vehicle identification number 1HSHXSJR2CJ624475 registered to Marck Gomez at 19122 East Elberland Street, West Covina, CA, 91792.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband fruits, or instrumentalities of violations of 18 U.S.C. § 549 (Removing Goods from Customs Custody); 18 U.S.C. 371 (Conspiracy); 18 U.S.C. § 545 (Smuggling Goods into the United States); and 18 U.S.C. § 542 (Entry of Goods by Means of False Statements) (collectively, the "SUBJECT OFFENSES"), namely:

a. Any counterfeit or duplicate high security bolt seals

b. All records related to FANNUM TRUCKS;

c. All communications between Marck Anthony Gomez and Allison Gonzales Montano regarding the diversion of cargo containers;

d. Any counterfeit items or prohibited food items deemed not inspected by CBP;

e. Data, records, documents, programs, applications or materials relating to the smuggling of goods , including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times of smuggled goods were bought, sold or otherwise distributed and any materials, documents, or records that are related to the sale, purchase, receipt, or possession of any smuggled goods, including books, receipts, photographs, bills of sale, shipping receipts, identification cards, bank statements, and correspondence discussing, requesting or confirming purchase, sale or shipment;

f. Tools, paraphernalia, or materials used as a means of packaging, selling, or distributing smuggled goods.

g. Any indicia of occupancy, residency, or ownership of the SUBJECT PREMISES and things described in the warrant, including forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

h. Items of personal property reflecting names, addresses, telephone numbers, or communications of members or associates involved in the smuggling activities, including personal telephone books, address books, telephone bills, photographs, videotapes, facsimiles, personal notes, cables, telegrams, receipts, and documents and other items;

i. Any bills and/or subscriber documents related to digital devices used to facilitate the SUBJECT OFFENSES;

j. United States currency, money orders, or similar monetary instruments over $1,000 or bearer instruments worth over $1,000 (including cashier's checks, traveler's checks, certificates of· deposit, stock certificates, and bonds);

k. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, rubber bands, plastic or shrink wrap, and plastic sealing machines;

l. Records, documents, programs, applications, or materials reflecting or relating to payment, receipt,

concealment, transfer, or movement of money, including but not limited to bank account records and other financial institution records, wire transfer records, receipts, safe deposit box keys and records, and notes;

m. Records, communications, information, documents, programs, applications, or materials relating to communications made or records submitted to U.S Customs and Border Protection concerning the importation of merchandise.

n. Records, communications, information, documents, programs, applications, or materials relating to communications made or records submitted to any/all customs house broker(s).

o. Records, communications, information, documents, programs, applications, or materials relating to communications made or records submitted to U.S Customs and Border Protection concerning the importation of merchandise.

p. For all digital devices, records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

q. For all digital devices, records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any digital devices used to facilitate the SUBJECT OFFENSES and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

r. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email or social media communications or other text or written communications sent to or received from any digital device;

s. Contents of any calendar or date book, including any calendars or date books stored on any digital devices;

t. Audio recordings, photographs, video recordings or still captured images on any digital device, phone memory cards, or other storage related to the purchase, sale, transportation, or distribution of controlled substances and listed chemicals or the collection, transfer or laundering of the proceeds of illegal activities;

u. GPS coordinates and other location information or records identifying travel routes, destinations, origination points, and other locations;

v. Any digital device used to facilitate the above listed violations and forensic copies thereof.

2. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

3. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal

digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

6. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Martina Doino, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security ("DHS"). Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI'), and have been so employed since December 2019.

2. I attended the HSI Criminal Investigator Training Program at the Federal Law Enforcement Training Center("FLETC"), in Glynco, Georgia. At FLETC, I received training in conducting criminal investigations into customs violations such as narcotics smuggling, interdiction, and distribution of controlled substances.

3. I am currently assigned to the Los Angeles Border Enforcement Security Taskforce ("LA BEST") in Los Angeles, California, and have been so assigned since August 2021. LA BEST is a multiagency task force aimed at identifying, targeting, and eliminating vulnerabilities to the security of the United States related to the Los Angeles/Long Beach seaport complex, as well as the surrounding transportation and maritime corridors. My responsibilities include the investigation of violations of federal criminal laws, including crimes involving money laundering, narcotics trafficking, smuggling, fraud, and immigration violations.

4. Prior to my tenure as a special agent, I was a police officer in Key Biscayne, Florida from February 2015 to May 2019.

From July 2018 to May 2019, I was a Task Force Officer ("TFO") on a High Intensity Drug Trafficking Area Task Force, where I participated in investigations into money laundering and drug trafficking crimes in South Florida. Throughout my law enforcement career, I have participated in numerous criminal investigations involving narcotics importation, exportation or distribution. Through these investigations, I am familiar with the methods and practices of drug users, drug traffickers, and drug manufacturers. I have also spoken at length with other HSI SAs and local law enforcement officers regarding methods of drug trafficking.

5. Through my investigations, my training and experience, and discussions with other law enforcement personnel, I have become familiar with the tactics and methods employed by controlled substance traffickers to smuggle and safeguard controlled substances, distribute controlled substances, and collect and launder the proceeds from the sale of controlled substances. These methods include, but are not limited to, the use of wireless communications technology, such as cellular telephones and prepaid cellular accounts; counter surveillance; false or fictitious identities; and coded or vague communications in an attempt to avoid detection by law enforcement.

II. PURPOSE OF AFFIDAVIT

6. This affidavit is made in support of an application for search warrants for the following:

a. 2014 Freightliner Truck model Cascadia bearing California (CA) license plate "FANNUM" with vehicle identification number 3AKJGLD51ESFK4321 registered to Marck Gomez at 19122 East Elberland Street, West Covina, CA, 91792 (the "**SUBJECT VEHICLE 1**"), as described more fully in Attachment A-1;

b. 2014 Navistar International Truck bearing California (CA) license plate "9G70806" with vehicle identification number 3HSDJSNR8EN033349 registered to Marck GOMEZ at 19122 East Elberland Street, West Covina, CA, 91792 (the "**SUBJECT VEHICLE 2**"), as described more fully in Attachment A-2;

c. A 2012 Navistar International Truck bearing California (CA) license plate "FANNUM1" with vehicle identification number 1HSHXSJR2CJ624475 registered to Marck Gomez at 19122 East Elberland Street, West Covina, CA, 91792 (the "**SUBJECT VEHICLE 3**"), as described more fully in Attachment A-3 (**SUBJECT VEHICLES 1, 2,** and **3** are referred to herein collectively as the "**SUBJECT VEHICLES**"); and

d. A cellular device with phone number 626-494-4942, subscribed to FANNUM TRUCKS LLC at 19122 East Elberland Street, West Covina, CA, 91792 (the "**SUBJECT DEVICE**") believed to be

used by Marck Anthony GOMEZ and FANNUM TRUCKS, as described more fully in Attachment A-4.

7. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 549 (Removing Goods from Customs Custody); 18 U.S.C. 371 (Conspiracy); 18 U.S.C. § 545 (Smuggling Goods into the United States); and 18 U.S.C. § 542 (Entry of Goods by Means of False Statements) (collectively, the "SUBJECT OFFENSES"), as described more fully in Attachment B. Attachments A-1, A-2, and A-3 and B are incorporated herein by reference.

8. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. Background on Cargo Container Shipments at the Ports of Los Angeles and the Cargo Swapping Smuggling Scheme

9. United States Customs and Border Protection ("CBP") is responsible for, among other things, the examination of merchandise entering the United States to ensure that it is admissible under and in compliance with United States laws, and the assessment and collection of taxes, fees, and duties on

imported merchandise. In order to properly assess fees, CBP relies on a self-reporting regime in which different custom brokers inform CBP about the contents of the cargo they are trying to import into the United States.

10. Importers must supply CBP with 10 data elements when bringing goods into the United States which includes: Seller, Buyer, Importer of Record number, Consignee number, Manufacturer/Supplier, Ship To party, Country of Origin, HTSUS number, Container stuffing location, and Consolidator/Stuffer name/address).

11. CBP has local and national targeting units that targets shipments that may yield prohibited items.

12. Once cargo has been selected for CBP examination, CBP will examine the contents of the cargo for discrepancies such as verifying whether the manifest is accurate, whether the goods have consistent country of origin markings, whether there are contraband or smuggled goods, as well as inspecting for environmental, and agricultural violations.

13. Once the shipment has been selected for further inspection, the container is brought to a Centralized Examination Site CES (CES) for further inspection. Containers are supposed to proceed directly to the CES after being selected for inspection.

14. The Port of Long Beach/Los Angeles handles about 40 percent of secondary inspections for the entire country. Due to the uniquely high volume at the Port of Long Beach/Los Angeles, the transportation of the containers selected for further

inspection is not always controlled by CBP. In fact, the transportation of some containers selected for inspection is controlled by the broker who filed the entry/importation paperwork. In Los Angeles, custom brokers are allowed to select their own trucking company to pick up the container and take it to a CES for further inspection. This type of drayage, which is the process by which a container is unloaded, is called broker controlled drayage. The broker controlled drayage process is unique to the Los Angeles and Long Beach port. No other domestic ports have this policy in place.

15. Once cargo containers are ready for transportation at their place of origin, a high security bolt seal is affixed on the doors of the container, by the carrier, to maintain its integrity and to prevent any unauthorized person from gaining access to the cargo. The purpose of the high security bolt seal is to ensure that the cargo inside the container is not compromised. Each high security bolt seal has its own unique identification number that is documented on several import documents. The high security bolt seal number is assigned by the vessel carrier that will transport the sea container to its destination. Below is a picture of a high security bolt seal.

16. On February 1, 2023, Customs and Border Protection ("CBP") discovered that cargo was missing from a container that had just arrived from China, and that the missing cargo was replaced, or swapped, with cargo that had clearly already entered the United States, some of which had already undergone CBP inspection.

17. This cargo swap was accomplished by using a fraudulent high security bolt seal which cloned the correctly manifested seal and its unique identification number and gave the appearance that the container had not been opened when it fact its contents had been removed and the fraudulent high security bolt seal installed.

18. Homeland Security Investigations ("HSI") opened an investigation to determine how the cargo swap occurred, what cargo was removed, and who was involved in orchestrating the breaking of the seal and removal of cargo in customs custody.

19. Since then, CBP has uncovered 102 more incidents of "cargo swapping." That is incidents, where cargo containers had

their high security bolts cut and the cargo inside removed before being inspected by CBP.

20. HSI investigators have uncovered the cargo swapping scheme is a direct result of the vulnerabilities within the customer broker drayage process at the Port of Long Beach, California.

21. As described above, CBP allows customs brokers to arrange their own transportation between the port terminals and the centralized examination stations (CES) where CBP conducts inspection on imported goods that have been selected for inspection.

22. HSI has found brokers, importers, and logistic companies are not honoring CBP's explicit instructions to deliver containers directly to the CES locations.

23. The investigation has uncovered that the containers are diverted during the drayage process to prevent customs inspections and bypass custom fees.

24. Instead of being brought to the CES, HSI has found that containers are brought to an offsite location, the seal is cut, the cargo is swapped out for recycled used items. A clone seal matching the numbers of the original seal is then placed on the container. The container is ultimately delivered to be inspected by CBP.

25. HSI has concluded the smuggling scheme is a widespread industry practice which undermines the Government's authority to inspect goods coming into the United States. As a direct result of this smuggling scheme the United States government is unable

to properly secure its borders from prohibited items and impose the appropriate custom duty fees.

26. Although the exact number of swapped cargo incidents are unknown due to the sheer volume of this practice, a conservative estimate of losses would be around $50,000 dollars per diverted container in lost custom fees and fines. Based on the over 100 documented incidents, HSI believes that the scheme has resulted in approximately $5,000,000 in lost revenue to the United States.

27. In March 2024, federal agents were able to determine the cloned seals were being imported via the international mail from China by targets of the investigation. Agents began a sophisticated operation that included intercepting the air parcels, documenting the seal number, and placing CBP holds that would trigger controlled drayage on the impacted shipping containers. This operation led to the identification of more than 40 air parcels containing approximately 88 cloned seals and 79 associated sea containers.

28. To date HSI has seized more than $ 50,000,000 worth of prohibited items that would have been diverted and entered the United States without inspection. The numbers continue to grow every day has more inspections are completed and items are discovered.

IV. SUMMARY OF PROBABLE CAUSE

29. HSI special agents have found a common thread in 12 cargo swapping incidents: Marck Anthony Gomez and Allison Gonzales Montano.

30. Law enforcement determined that Gomez owns and operates FANNUM TRUCKS LLC which is the listed carrier in several cargo swapping events. Gonzales-Montano is believed to be a driver for FANNUM TRUCKS LLC.

31. Between February 2023 and April 2024, FANNUM TRUCKS LLC has been listed as the trucking company responsible for transporting cargo containers, using the **SUBJECT VEHICLES**, in 12 cargo swap incidents, incidents in which cargo containers have arrived at CBP inspection sites with tampered seals.

32. Phone tolls of the **SUBJECT DEVICE** show frequent communication with the truck drivers, including Gonzales-Montano, responsible for transporting the swapped cargo containers during the period of time when the cargo containers have been illegally taken from Custom's custody.

V. STATEMENT OF PROBABLE CAUSE

A. SUBJECT VEHICLE 3 Carries Out A Cargo Swap Event On September 18,2023

33. I know from reviewing law enforcement reports that on August 26, 2023, container number TGBU5135370 (the "5310 Container") arrived at the Port of Long Beach, California from Nansha, China. On August 29, 2023, CBP placed an examination hold to inspect the contents of the 5310 Container.

34. On September 19, 2023, the 5310 Container arrived at the Price Central Examination Station ("CES") located in Carson, California at approximately 12:14 a.m.

35. According to the terminal out gate ticket[1] from the Long Beach Terminal, the 5310 Container was picked up at the Long Beach Terminal inside the Port of Long Beach on September 18, 2024, at approximately 7:19 p.m.

36. Based on my review of the terminal in gate ticket[2] from the Price CES, I know that the container took four hours and fifty-four minutes to reach the PRICE CES facility. The total distance between the locations is approximately 11 miles, with an estimated 25-minute drive time at peak traffic. The fact that it took the 5310 Container over four hours to reach the Price CES suggests to me that it was illegally diverted to a third location prior to it being delivered to the Price CES.

37. On September 19, 2023, CBP inspected the contents of the 5310 Container and found boxes containing FFG branded Facemasks and medical gowns as well as CBP inspection tape. Based on my knowledge of the investigation, I have seen this type of cargo used in many cargo swapping events. I believe that this filler cargo is cargo specifically placed in containers for the sole purpose of filling it back up after the original cargo has

[1] A terminal out gate ticket is a document provided to truck drivers when exiting a terminal that includes the container number in their possession and time stamps.

[2] A terminal in gate ticket is a document provided to truck drivers when entering a terminal that includes the container number in their possession and time stamps.

been swapped out. I believe that the filler cargo has little to no value. I also know that the presence of old CBP inspection tape in a cargo container that was not yet supposed to have been inspected indicates that the cargo inspection process had been compromised.

38. I reviewed records provided by PRICE CES showing that the truck driver for the 5370 Container was Allison Gonzalez-Montano. FANNUM TRUCKS LLC was listed as the trucking company responsible for the transportation of the 5370 Container using **SUBJECT VEHICLE 3.**

39. Based on records from PRICE CES, I know that GONZALEZ-Montano was driving **SUBJECT VEHICLE 3.** Based on my knowledge of the investigation, Gonzalez-Montano has been linked to approximately eight cargo swap events as the driver of a cargo container that was later determined to be swapped. Including the above-described cargo swapping event which occurred on September 18-19, 2023.

40. I reviewed phone tolls of the **SUBJECT DEVICE** which showed that Gonzalez-Montano was in contact with the **SUBJECT DEVICE** during the September 18, 2023, cargo swapping event. Based on my knowledge of the investigation, I believe the fact that Gonzalez-Montano was in communication with the **SUBJECT DEVICE** while he was illegally diverting the cargo container means that there is like to be evidence of the SUBJECT OFFENSES on the **SUBJECT DEVICE.**

B. SUBJECT VEHICLE 1 Is Used In Another Cargo Swapping Event on January 17, 2024

41. I know from reviewing law enforcement records, that on January 8, 2024, Container number RJCU2022275 (the "2275 Container") arrived at the Port of Long Beach, California aboard SM Shanghai vessel from Shanghai, China. Prior to its arrival, on January 4, 2024, CBP placed an examination hold to inspect the contents of that container.

42. On January 17, 2024, the 2275 Container arrived at the Price CES at approximately 10:55 p.m.

43. According to the terminal out gate ticket, I know that the 2275 Container was picked up at the SSA Marine Terminal inside the Port of Long Beach on January 17, 2024, at approximately 4:08 p.m.

44. Based on my review of the terminal in gate ticket from the Price CES, I know that the container took almost six hours and forty-seven minutes to reach the Price CES. The total distance between the Price CES and the Fenix Marine Terminal is approximately 11 miles, with an estimated 25-minute drive time at peak traffic. The fact that it took the 2275 Container over six hours to reach the Price CES suggests to me that it was illegally diverted to a third location prior to it being delivered to the Price CES.

45. I know from reviewing law enforcement reports that on January 19, 2024, CBP inspected the contents of the container and found boxes of disposable face masks and blood collection tubes. Additionally, the 2275 Container arrived in a non-active reefer container. A reefer container is a refrigerated container used

to maintain cold temperatures when transporting items needing refrigeration. Based on my training and experience, I believe that economically it would not make sense to transport items that do not need refrigeration in a refrigerated container. Based on the foregoing, I believe that the original cargo, which probably needed refrigeration, had likely been swapped and replaced before CBP inspection.

46. According to the documents provided to law enforcement by PRICE CES, the truck driver for the 2275 Container was Mark Gomez.

47. On the container information sheet provided by PRICE CES, which I reviewed, FANNUM TRUCKS LLC was the trucking company listed for the delivery of the 2275 Container. GOMEZ was listed as the driver and **SUBJECT VEHICLE 1** was listed as the vehicle used during the delivery of the 2275 Container.

C. SUBJECT VEHICLE 2 Is Used During Another Cargo Swap Event on March 28, 2024

48. Based on law enforcement reports, on March 21, 2024, federal agents inspected container number TCNU6659916 at the PRICE CES facility (the "9916 Container"). The inspection uncovered multiple suspected counterfeit items in the 9916 Container such as BIC lighters, plastic bongs, and food items. The 9916 Container, however, was manifested as containing "Stainless steel cups."

49. On March 26, 2024, the Honorable United States Magistrate Judge Jaqueline Chooljian authorized a search warrant,

in case number 2-24-MJ-1745, to place a tracker inside the 9916 Container and to search a location (1365 Darius Ct, City of Industry) if the 9916 Container arrived at that location.

50. Based on law enforcement reports, I know that on March 28, 2024, at approximately 11:52 a.m. the 9916 Container was out gated at the Fenix Marine Terminal by an unidentified individual utilizing **SUBJECT VEHICLE 2**. Federal agents observed that the driver of **SUBJECT VEHICLE 2** was a bald Hispanic male later identified, via comparison with his California Driver's license picture, as Gomez.

51. Agents spoke with the Terminal employees, who stated Exclusive Logistics Trucking made the reservation to pick up the 9916 Container.

52. At approximately 12:40 p.m., the 9916 Container left the terminal affixed to **SUBJECT VEHICLE 2** which was driven by GOMEZ. Instead of proceeding to the PRICE CES, as required by CBP, federal agents surveilled the 9916 Container drive to the City of Industry, California.

53. At approximately 2:16 p.m., the 9916 Container arrived at a commercial warehouse located at 15736 East Valley Blvd. and backed up to the loading dock number six.

54. Law enforcement observed GOMEZ step out of the truck and walk toward the parking lot. GOMEZ was later seen speaking to an unidentified Asian male, later identified as Hexi WANG, who the investigation reveals was involved in several other cargo swapping events.

55. At approximately 2:45 p.m., the 9916 Container arrived at 1365 Darius Court, City of Industry, California. Federal agents observed GOMEZ park the 9916 Container on the side of the street closest to the loading docks. GOMEZ remained in the driver seat of **SUBJECT VEHICLE 2**.

56. At approximately 4:10 p.m., the 9916 Container arrived at the Price CES facility. Agents observed GOMEZ pull off to the side of the road and walk to the back of the 9916 Container. GOMEZ was observed touching and taking photos of the seal with a cellphone, which I believe is the **SUBJECT DEVICE**.

57. At approximately 4:30 p.m., GOMEZ approached the guard gate at the PRICE CES warehouse and was observed speaking with a PRICE employee. GOMEZ appeared nervous and kept pacing back and forth. GOMEZ brought the PRICE employee to the rear of the 9916 Container and pointed to the seal. A short while later, the 9916 Container was accepted by PRICE employees. CBP Officer Robert Adams approached GOMEZ at the Price CES lot near the guard gate and had a brief conversation with him.

58. According to CBP Officer Adams, during that conversation, GOMEZ told CBP Officer Adams that he wanted them to know about an issue with the seal. GOMEZ stated that the seal had broken off when he backed up the chassis in Carson while he was "swapping out" with another driver.

59. GOMEZ told CBP Officer Adams that he did not pick up the 9916 Container at the Port of Long Beach and that another one of his employees had picked it up. GOMEZ told CBP Officer Adams that he had placed one of his personal GLOBAL INDUSTRIAL seals on

the container in order to secure it. GOMEZ then gave CBP Officer Adams his phone number of 626-494-4942, which I believe to be the **SUBJECT DEVICE.**

60. Based on the reports of surveillance of the 9916 Container, which I reviewed, I know that GOMEZ picked up the 9916 Container from the Port and never met with another driver to swap.

61. I reviewed subscriber records for the **SUBJECT DEVICE** obtained from T-Mobile. The records show the **SUBJECT DEVICE** was registered to FANNUM TRUCKS LLC, at 19122 East Elberland Street, West Covina, California 91792.

VII.TRAINING AND EXPIRIENCE ON SMUGGLING

62. Based on my training and experience, I am familiar with the methods employed in smuggling operations and the patterns employed by smuggling organizations. I have also spoken with other experienced agents and other law enforcement officers about their experiences and the results of their investigations and interviews. I am knowledgeable in the methods and modes of smuggling operations and the language patterns of these groups. I have become familiar with the methods of operation typically used by smugglers. Based on my training, experience, my conversations with other law enforcement officers, and my knowledge of this investigation and others, I am aware of the following.

63. Smugglers frequently conduct their illegal activities inside of secure locations, which are private, but to which they have ready access; therefore, I believe that SUBJECT PREMISES 1,

2, 3 are likely to be areas where persons who are engaged in smuggling are located and conduct their operations.

64. Smugglers will frequently keep the smuggled goods supplier and customer records, and other items relating to their smuggling activities at their residences (including garages and outbuildings on their properties), businesses, and other secure areas, such as storage lockers.

65. Smugglers also conceal items related to their crimes in vehicles, including vehicles outside of their residences, or Businesses so that they have ready access to them and so that they can hide them from law enforcement, including law enforcement officers executing search warrants at their residences or businesses.

66. Smugglers will often have secret show rooms inside a business or residence to showcase the smuggled goods available. Including in locked safes, drawers, and filing cabinets.

67. Smugglers will often receive goods on a regular basis. Such smugglers will thus have an "inventory" which will fluctuate in size depending on the demand for the product.

68. Smugglers often use one or more telephones, pagers, or other digital devices to negotiate times, places, schemes, and manners for importing, possessing, concealing, manufacturing, and distributing smuggled goods, and for arranging the proceeds from the sale of the smuggled goods. Additionally, I know that professional smugglers depend upon maintaining both long-distance and local contacts with both suppliers and those down the organizational chain, to the local distributors.

69. Data contained on digital devices used by smugglers often include, among other things, records of telephone calls, text messages, and e-mail and social media communications between the Smugglers and the co-conspirators; Global Positioning System ("GPS") information and other location information that can help identify stash locations, meeting places, and smuggling routes; and identifying information about the smugglers and co-conspirators, such as contact lists, calendar appointments, and photographs or videos.

70. Individuals involved in smuggling often have in their possession – that is, on their persons, at their residence, and/or at their stash houses – firearms, including handguns, pistols, revolvers, rifles, shotguns, machine guns and/or other weapons, as well as ammunition and ammunition components, that are used to protect and secure the smuggling property.

71. Individuals involved in smuggling typically pay or receive large sums of money for goods. Therefore, smugglers typically have significant amounts of cash on hand, as proceeds of sales, to purchase their own supplies, or as profits from their smuggling activities (such as profits from sales or profits from the transportation of smuggled goods).

72. Smugglers also often maintain in their residences, businesses or vehicles documents relating to their communication devices, in the form of receipts, bills, telephone and address books, and other books and papers which reflect, among other things, the names, addresses, and/or telephone numbers of their

customers, co-conspirators, and associates in the smuggling organization.

73. Individuals involved in smuggling goods can provide goods on credit to trusted distributors in their organization and can obtain smuggled goods from their suppliers on credit. Therefore, I am aware that individuals involved in smuggling goods maintain books, records, customer lists, receipts, notes, ledgers, and other papers relating to the transportation, receipt, ordering, sales, and distribution of goods, proceeds, and equipment, and that such documents may be in code to attempt to thwart law enforcement.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

74. As used herein, the term "digital device" includes the **SUBJECT DEVICE.**

75. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary

directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously

develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

76. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data in a short period of time for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

77. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

V. CONCLUSION

78. For all the reasons described above, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of Subject offenses will be found in the **SUBJECT DEVICE** and **SUBJECT VEHICLES**, as described in Attachments A-1, A-2, A-3, and A-4.

Subscribed to and sworn before me
this 21st day of June, 2024.

HONORABLE ALKA SAGAR
UNITED STATES MAGISTRATE JUDGE